REMARKS

After entry of the foregoing amendments, Claims 1-55 are pending in this application. Independent Claims 1, 14, 27, 33, 34, 35, 40, and 47, and dependent Claims 29, 30, and 31 have been amended by the present Response. Applicant respectfully submits that no new matter has been added by the foregoing amendments. Reconsideration of the application, as amended, is requested.

Objections to the Specification

In the Non-final Office Action dated January 12, 2007, the Specification was objected to due to informalities. In particular, the Office Action contended that the word "cyphertext" is misspelled in paragraph [0007].

In Response, the Applicant notes that this typographical error was not present in the Specification as originally filed, but instead first appeared in the publication of the present patent application. However, the Applicant has amended paragraph [0007] to correct the typographical error. The term "cyphertexi" has been corrected to now read "cyphertext." Accordingly, the Applicant respectfully contends that the informalities in the Specification that were pointed out by the Office Action have been corrected.

Objections to the Claims

In the Non-final Office Action, Claim 37 was objected to because Claim 33 currently depends from Claim 37. The Office Action contends that this dependency is incorrect because Claim 33 is a claim to further limit an encoder and Claim 37 is a claim to further limit a method claim.

In Response, Claim 33 has been amended to now depend from Claim 27 rather than Claim 37. Accordingly, the Applicant respectfully contends that any informalities with respect to Claims 33 and 37 have been corrected and that the claims are in condition for allowance.

Rejection of Claims 1-55 Under 35 U.S.C. § 102(e)

In the Non-final Office Action, Claims 1-55 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Application No. 2003/0091184 to *Chui* ("*Chui*"). However, the Applicant respectfully contends that the amended claims are patentable over *Chui*.

Chui is directed to a system and method for real-time secure communication based on applying multi-level wavelet transforms to data and then encrypting the results of each level of the multi-level wavelet transforms (*See Chui* at paragraphs [0056] – [0058]). A wavelet transform, or a discrete wavelet transform (DWT) is applied to data in order to decompose the data into a low-frequency band and a high-frequency band (*See Chui* at paragraph [0056]). The low-frequency band, which results from the DWT, is then encrypted using an encryption key set (*See Chui* at paragraph [0057]). A second wavelet transform is then applied to the encrypted low-frequency band to produce a second level low-frequency band and a second level high-frequency band (*See Chui* at paragraph [0056]). By repeating this process "n" times, the original signal is decomposed into the sum of "n" high frequency bands and the "nth" low frequency band (*See Chui* at paragraph [0056]). At each level of the decomposition, the coefficients of the low-frequency band may be encrypted by using an encryption key set that is unique to the particular level of the decomposition (*See Chui* at paragraph [0057]). Following the transfer or communication of the encrypted data, corresponding decryption key sets and inverse wavelet transforms (IDWT) are then utilized by a transform-decryption system in order to reproduce the original data (*See Chui* at paragraph [0063]).

In order to perform the DWT and IDWT, two sets of filters may be used in *Chui*, both of which operate within a real field (*See Chui* at paragraphs [0066] – [0071]). For each DWT operation performed, a distinct set of wavelet transform coefficients, or scaling coefficients for the low-frequency band, is produced (*See Chui* at paragraph [0074]). These wavelet transform coefficients are encrypted by using an encryption key set (*See Chui* at paragraph [0075]). A symmetric key encryption technique such as an affine cipher is utilized to encrypt the wavelet transform coefficients at each level of the decomposition (*See Chui* at paragraphs [0076] and [0091].)

Patentability of the Independent Claims

While *Chui* appears to perform a combination of a wavelet transform and an encryption technique on an input signal, *Chui* performs these two steps as distinct operations. In marked contrast to *Chui*, the system described in independent Claim 1 specifically recites an encryption system operable to "perform an inverse wavelet transformation over a finite field on said plaintext to produce cyphertext." In other words, the cyphertext is produced by the performance of an inverse wavelet transformation. *Chui* fails to teach or suggest a system operable to "perform an inverse wavelet transformation over a finite field on said plaintext to produce cyphertext." In marked contrast, *Chui* applies an encryption key set to the transform coefficients of a discrete wavelet transform in order to produce an encrypted cyphertext. No encryption is performed by *Chui* unit the discrete wavelet transform is completed. Accordingly, *Chui* fails to anticipate each of the elements of independent Claim 1. Therefore, the Applicant respectfully asserts that independent Claim 1 is allowable over *Chui*.

Although Applicant contends that independent Claim 1 is allowable over *Chui*, in order to clarify the claims of the present patent application, independent Claim 1 has been amended to specifically recite that the encryption system is operable to "encrypt said plaintext at least in part by performing an inverse wavelet transformation over a finite field on said plaintext to produce cyphertext." As amended, Claim 1 recites the use of an inverse wavelet transform in the encryption of the plaintext. As discussed above, *Chui* fails to teach or suggest an encryption system operable to "encrypt said plaintext at least in part by performing an inverse wavelet transformation over a finite field on said plaintext to produce cyphertext." The system and method of *Chui* do not encrypt any data with a discrete wavelet transform. Instead, *Chui* encrypts the transformed coefficients following the application of a discrete wavelet transform (*See Chui* at paragraphs [0057] and [0075]). In other words the discrete wavelet transform or filter in *Chui* is not part of the block cipher or cyclic key that is utilized to encrypt data. In fact, *Chui* appears to recognize that the wavelet transformation step and the encryption step are distinct from one another. For example, *Chui* states that each box **114** labeled "E" in FIG. 2A represents a symmetric key encryption operation, and each box **116** labeled "DWT" in FIG. 2A represents a DWT operation on the input data received by that DWT box (*See Chui* at paragraph [0061]). Accordingly, *Chui* fails to teach or suggest an encryption system operable to "encrypt

said plaintext at least in part by performing an inverse wavelet transformation over a finite field on said plaintext to produce cyphertext," as recited by independent Claim 1.

Additionally, *Chui* fails to teach or suggest an inverse wavelet transformation or a wavelet transformation that operates over a "finite field," as recited by independent Claim 1. Instead, the two discrete wavelet transformations or filters taught by *Chui* operate over a "real field" (*See Chui* at paragraphs [0066] – [0071]). In other words, the coefficients of the filters taught by *Chui* are real numbers. The *Chui* filters operate within the real or complex number domain and then scale or normalize the results or output into the integer domain. Such scaling or normalization results in a decrease in the accuracy of the filter output. In marked contrast, independent Claim 1 recites a transformation over a "finite field" rather than a transformation over a "real field." *Chui* fails to teach or suggest a transformation over a "finite field," as recited by independent Claim 1.

For at least the reasons set forth above, *Chui* fails to teach or suggest an encryption system operable to "encrypt said plaintext at least in part by performing an inverse wavelet transformation over a finite field on said plaintext to produce cyphertext." Therefore, the Applicant respectfully asserts that amended independent Claim 1 is allowable over *Chui*. Because Claims 2-13 depend from independent Claim 1, those claims are likewise allowable as a matter of law as depending from an allowable base claim, notwithstanding their independent recitation of patentable features.

Independent Claims 14, 27, 34, 35, 40, and 47 have been amended in the same manner as independent Claim 1. Accordingly, independent Claims 14, 27, 34, 35, 40, and 47 also recite, among other things, that the encryption system is operable to "encrypt said plaintext at least in part by performing an inverse wavelet transformation (or wavelet transformation in some of the claims) over a finite field on said plaintext to produce cyphertext." The Applicant respectfully asserts that all remarks addressing the novelty of Claim 1 are also applicable to amended Claims 14, 27, 34, 35, 40, and 47. Therefore, the Applicant asserts that Claims 14, 27, 34, 35, 40, and 47 are allowable for the same reasons set forth above with respect to Claim 1. Further, because Claims 15-26, 28-33, 36-39, 41-46, and 48-55 depend from independent Claim 14, 27, 35, 40, and 47 respectively, the Applicant asserts those claims are also allowable as a matter of law as depending from an allowable base claim, notwithstanding their independent recitation of

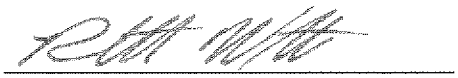
patentable features.

CONCLUSION

The Applicant believes that each matter raised by the Examiner has been addressed. Allowance of the claims is respectfully solicited. It is not believed that extensions of time or fees for addition of claims are required beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 CFR §1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 19-5029.

If there are any issues which can be resolved by telephone conference or an Examiner's Amendment, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,



Rhett S. White
Attorney for Applicant
Registration No. 59,158

Date: April 6, 2007

SUTHERLAND ASBILL & BRENNAN, LLP
999 Peachtree Street, NE
Atlanta, GA 30309-3996
(404) 853-8233
(404) 853-8806 (fax)
SAB Docket No.: 23952-0052